

Date: Sat, 14 Aug 93 04:30:00 PDT
From: Packet-Radio Mailing List and Newsgroup <packet-radio@ucsd.edu>
Errors-To: Packet-Radio-Errors@UCSD.Edu
Reply-To: Packet-Radio@UCSD.Edu
Precedence: Bulk
Subject: Packet-Radio Digest V93 #239
To: packet-radio

Packet-Radio Digest Sat, 14 Aug 93 Volume 93 : Issue 239

Today's Topics:

Change of Newsgroup (2 msgs)
DC metro area packet buffs?
MFJ-1270 LM-324 replacement
packet radio encryption

Password verification vs. encryption (was Re: packet radio encryption)

Send Replies or notes for publication to: <Packet-Radio@UCSD.Edu>
Send subscription requests to: <Packet-Radio-REQUEST@UCSD.Edu>
Problems you can't solve otherwise to brian@ucsd.edu.

Archives of past issues of the Packet-Radio Digest are available
(by FTP only) from UCSD.Edu in directory "mailarchives/packet-radio".

We trust that readers are intelligent enough to realize that all text
herein consists of personal comments and does not represent the official
policies or positions of any party. Your mileage may vary. So there.

Date: Thu, 12 Aug 93 13:57:55 EST
From: dog.ee.lbl.gov!overload.lbl.gov!agate!howland.reston.ans.net!torn!nott!
cunews!revcan!balsam!pinetree!gordon@network.ucsd.edu
Subject: Change of Newsgroup
To: packet-radio@ucsd.edu

sfarlow@NeoSoft.com (Stephen Farlow) writes:

> I am not too happy to hear about the discontinuance of rec.radio.amateur.
> packet nad putting it into rec.radio.amateur.digital.misc.
> Packet is a very specific term and I don't want to have to read through
> messages about all other sorts of digital modes to sort out packet ones.
> WHY THE CHANGE ?
> I urge you to leave rec.radio.amateur.packet alone and put those other
> digital modes into the new group !

The change is because part of the CFV for the rec.radio.amateur re-org
made provision for the removal of "old" groups made redundant under the

new group structure. Of those who voted, a majority voted in favour of creating rec.radio.amateur.digital.misc. The charter of the group includes packet among the other digital modes, so rec.radio.amateur.packet will be rmgroup'd sometime in September.

Once rec.radio.amateur.packet is rmgroup'd and you've had a chance to find out just what sort of traffic is in rec.radio.amateur.digital.misc and it turns out that there's high traffic of messages about all the various digital modes and reading packet related messages is a pain, put forward an RFD to create rec.radio.amateur.digital.packet group. If the readership supports it's creation, then you'll have your packet group.

Cheers!

--G

--

Internet: gordon@pinetree.org		Guillotine operators
UUCP: ...!pinetree!gordon		get severance pay.
Packet: VE3XGD@VE3JF		* VE3XGD *
Gordon's Pinetree - Ottawa, Ontario, Canada - +1 613 526 0702 - v32bis/v42bis		

Date: Fri, 13 Aug 1993 12:06:11 GMT

From: swrinde!cs.utexas.edu!csc.ti.com!tilde.csc.ti.com!ra.csc.ti.com!

fstop.csc.ti.com!sbrown@network.ucsd.edu

Subject: Change of Newsgroup

To: packet-radio@ucsd.edu

In article <1993Aug12.192800.7298@nntpd2.cxo.dec.com> segrest@bobseg.enet.dec.com
() writes:

> It seems to me that a vote was held to make this decision... I wonder where
> everyone was when that happened...
>
> If you voted, you got your chance to participate in the decision process. If
> you failed to vote, you forfeited your right to gripe. Why don't you stop
> your whining.
>
> There are a set of rules that govern the creation of a news group and when
> they allow we will have another vote. Perhaps more people will participate
> and we will get a different result.
>
> --
> Bob Segrest
> segrest@bobseg.enet.dec.com

Here, Here! I second that. Right on! Yes-s-s! < Other indications of agreement and support. >

```
*****
| Steve Brown, WD5HCY          |          |
| sbrown@charon.dseg.ti.com    | Simplicate |
| wd5hcy@wd5hcy.ampr.org       | and add    |
| [44.28.0.61]                 | lightness. |
| wd5hcy@kf5mg.#dfw.tx.usa.na |          |
*****
```

Date: Sat, 14 Aug 1993 03:32:37 GMT
From: sytex!jim@uunet.uu.net
Subject: DC metro area packet buffs?
To: packet-radio@ucsd.edu

Any packet buffs in the DC metro area? Looking for guidance, peeking at rigs, and big brothers ...

jim

jim@sytex.com (Jim Arnold)
Access <=> Internet BBS, a public access internet site
Sytex Communications, Arlington VA, 1-703-528-4380
-- Internet Access for the rest of us...

Date: Fri, 13 Aug 93 16:26:09 MST
From: dog.ee.lbl.gov!overload.lbl.gov!agate!howland.reston.ans.net!
vixen.cso.uiuc.edu!uwm.edu!cs.utexas.edu!asuvax!ennews!stat!aznet!
dan@network.ucsd.edu
Subject: MFJ-1270 LM-324 replacement
To: packet-radio@ucsd.edu

zardoz@ornews.intel.com (Jim Garver) writes:

>
> What is the part number for the chip with a faster slew rate than the
> LM-324 op amp used in the MFJ-1270 TNC-2 clone? This mod is supposed
> to allow use of the higher serial port baud rates. Thanks.
> --
> WA7LDV zardoz@ornews.intel.com

TL087 or TL088

73 de Dan N7MRP

Internet: dan@aznet.stat.com
Ax.25: n7mrp@n7mrp.az.usa.na
Voice: (602) 956-2566

Date: Fri, 13 Aug 1993 06:16:47 +0000
From: usc!howland.reston.ans.net!agate!doc.ic.ac.uk!warwick!qmw-dcs!qmw!demon!
llondel.demon.co.uk!dave@network.ucsd.edu
Subject: packet radio encryption
To: packet-radio@ucsd.edu

How about looking at it the way UK authorities do: they make a distinction between encoding a signal to facilitate transmission and encrypting a signal to prevent others from reading it.

In the first category comes things like the scramblers used on G3RUH/K9NG modems (and others no doubt), using PKZIP to compress a file so it takes less bandwidth, 7plus and UUcode etc. The fact that most of these make it difficult for someone else to read the contents is purely coincidental.....

Even ASCII is a code.....

Dave

```
*****
* G4WRW @ GB7WRW.#41.GBR.EU AX25      *   You think *you* have problems?   *
* dave@llondel.demon.co.uk Internet *   What do you do if you *are*       *
* g4wrw@g4wrw.ampr.org      Amprnet *   a manically depressed robot??    *
*****
```

Date: Fri, 13 Aug 1993 19:50:39 GMT
From: dog.ee.lbl.gov!overload.lbl.gov!agate!howland.reston.ans.net!
vixen.cso.uiuc.edu!sdd.hp.com!nigel.msen.com!well!moon!pixar!mongo!
bruce@network.ucsd.edu
Subject: Password verification vs. encryption (was Re: packet radio encryption)
To: packet-radio@ucsd.edu

While encryption to obscure meaning is prohibited, it is not prohibited to use something like a zero-knowledge proof to verify a password. Note that a zero-knowledge proof communicates information about the password without communicating the password itself, and the information is not obscured.

It works this way:

Prover: I know the secret number.

Verifier: Oh yeah? Well, what's the remainder when you divide the
secret number by 1958?

Prover: It's 22.

Verifier: OK, I'm 95% sure you know the secret number. Now,
what's the remainder when you divide the secret number
by 111?

Prover: It's 105.

Verifier: OK, I'm 99.99% sure you know the secret number. That's
good enough, so you can log in now.

The next time, the verifier will use different divisors so that anyone
who knows these two won't have any useful information.

In practice, the questions are a bit more complicated, and there are rules
to use in forming the number and the questions so that no information that
would be valuable to a system cracker will be communicated.

Bruce Perens KD60TD

Date: 13 Aug 93 18:42:25 GMT

From: psinntp!newsserver.pixel.kodak.com!kodak!eastman!isctsae!braun@uunet.uu.net
To: packet-radio@ucsd.edu

References <CBHz15.15LE@hawnews.watson.ibm.com>, <2472d8\$ld7@apple.com>,
<CBJvHv.FM3@dptspd.sat.datapoint.com>om
Subject : Re: Types of gateways (was Re: Internet <-> packet gateway near)

Let's get REAL, Appletalk has converted over to encrypted passwords.
Why can't this be implemented in the TCP/IP environment?
Are we waiting for the lan based community? shouldn't we do this
ourselves?

Just some network engineers ramblings about etherpeek and passwords :-).

--
Curtis Braun (curtis@computronics.com) (n2hkd) braun@telstar.kodak.com
Computronics, POBOX 1002 Fairport, NY 14450
Guest@Digital Telstar, Network Operations Center Kodak

End of Packet-Radio Digest V93 #239
